

Fig 1

FIG. 1

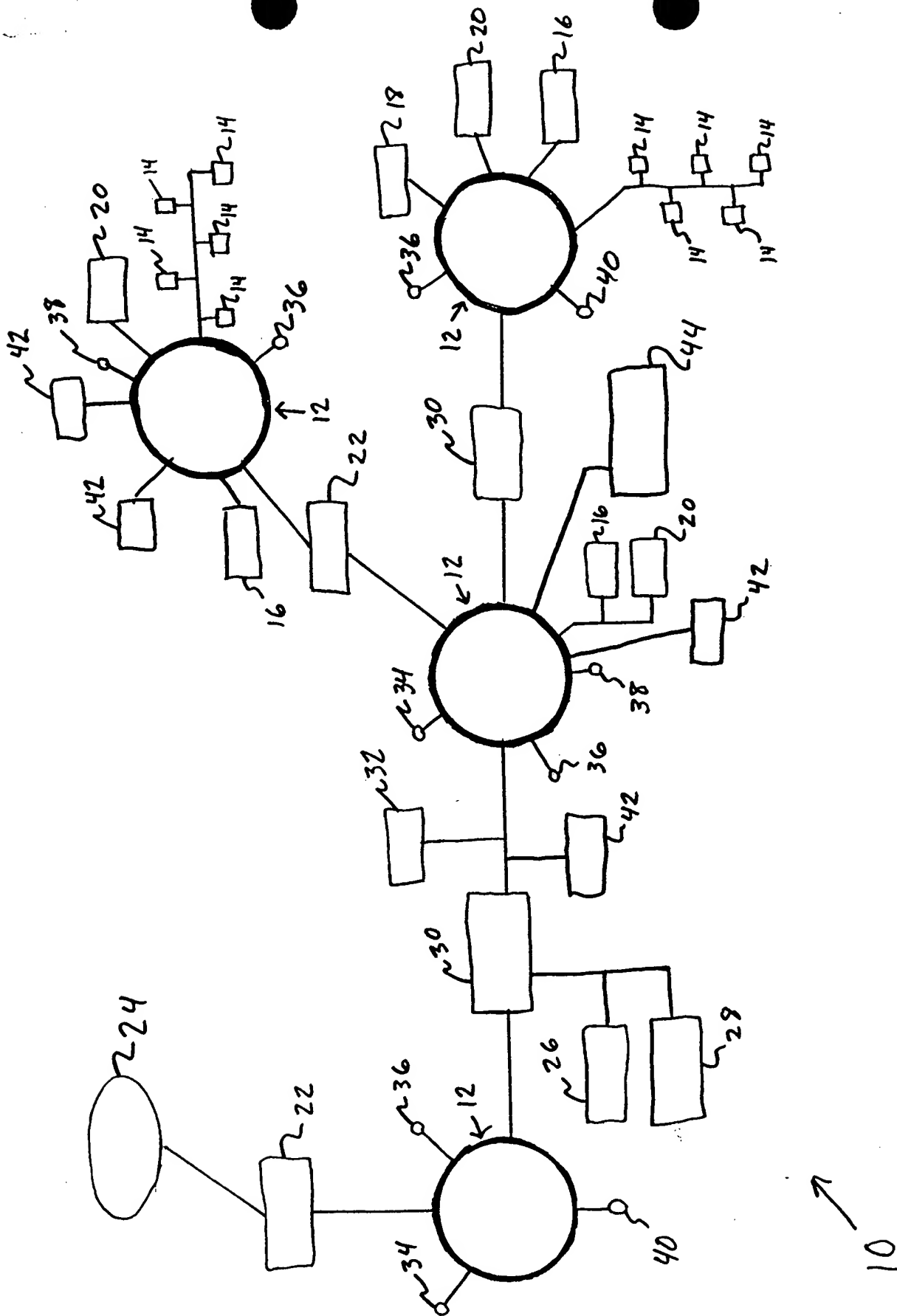


Figure 2

Figure 2

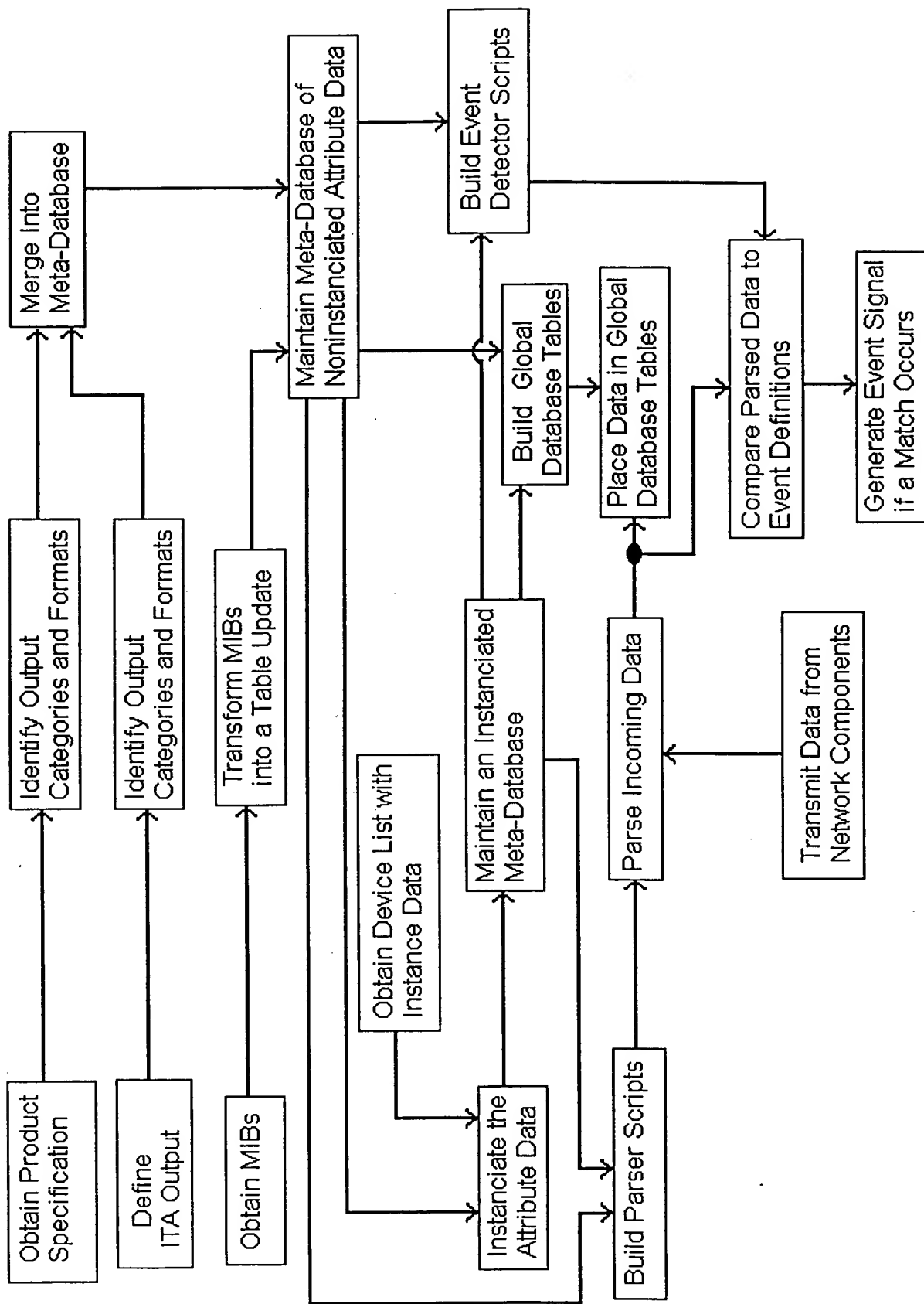


Figure 3

TOP SECRET

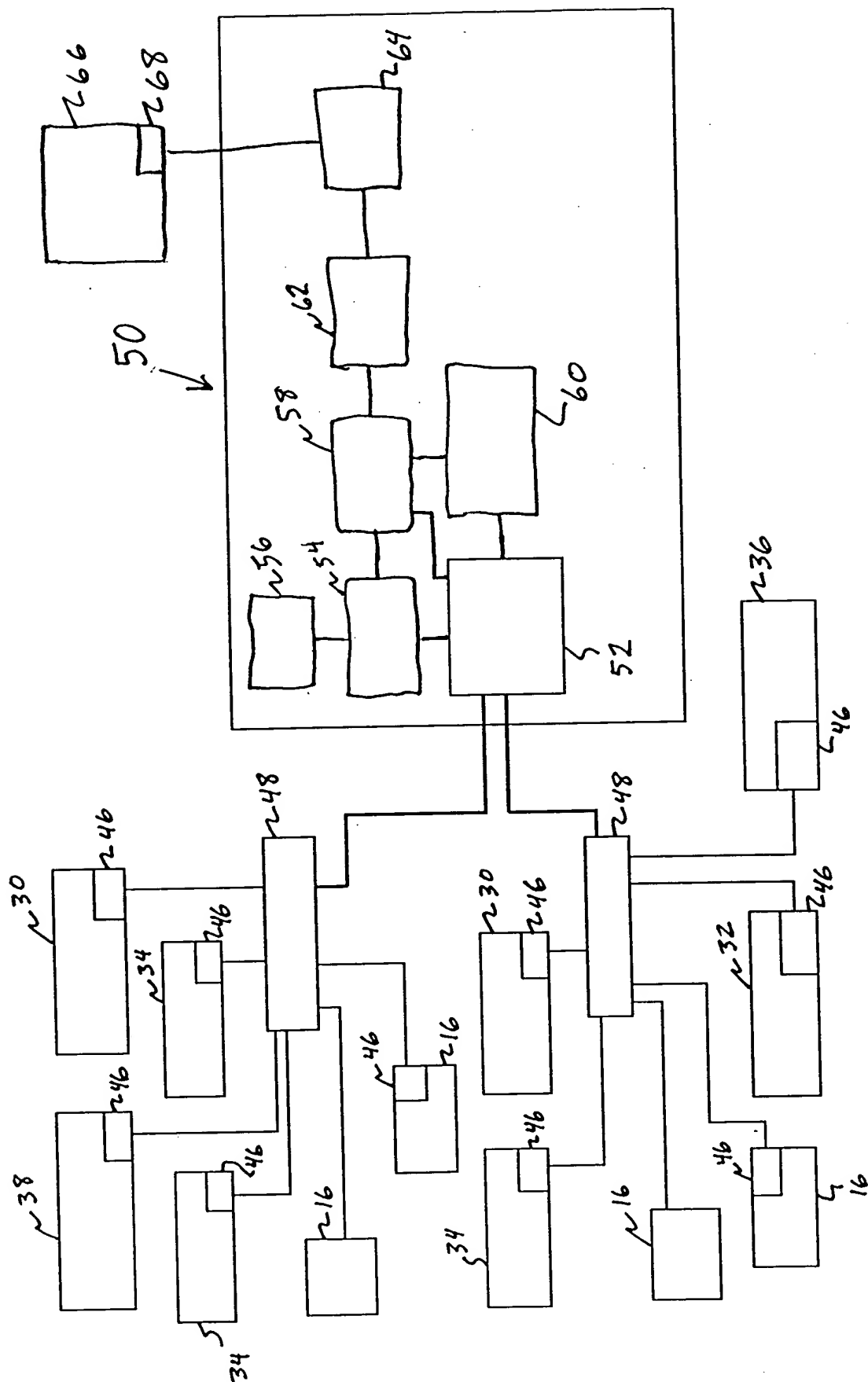


Figure 4

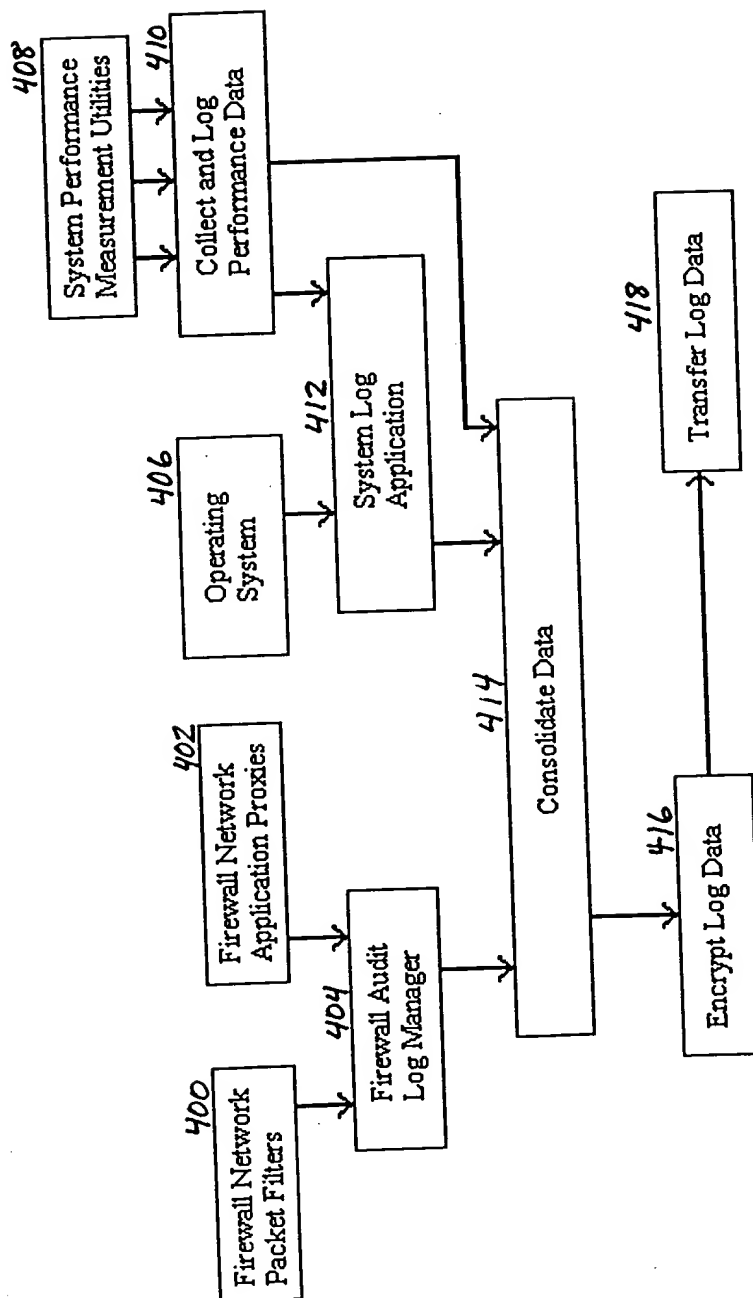


Figure 5

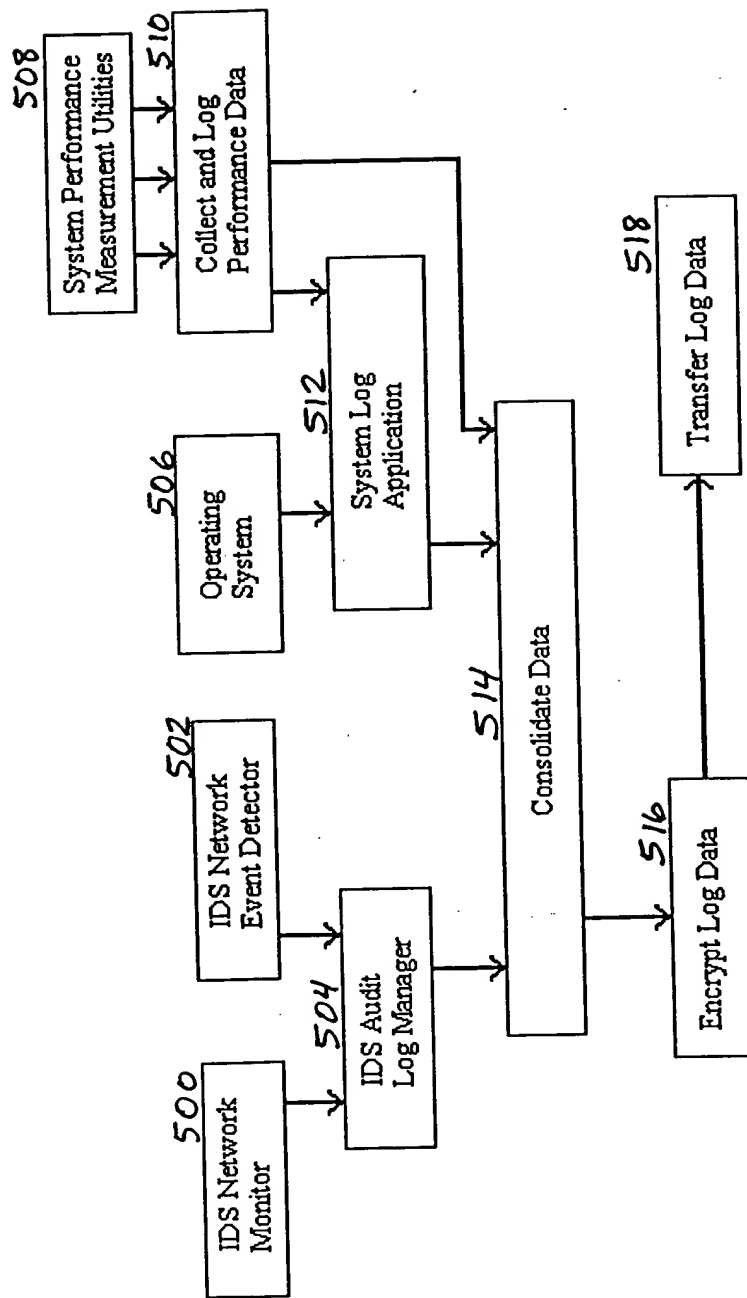


Figure 6

700

Transaction Table		stream id	conditional
transaction id	description	system type id	
X200154	A record of a network transaction through a CyberGuard firewall	T100001	(\$Action == "T")
X317189	A record of CPU percent idle, percent system, percent I/O, and percent user	T100001	TRUE

702

System Type Table		load	revision	patch
system type id	model	version		
T100001	CyberGuard Corp	2	2.3	11

704

Stream Table		end of record	end of field
stream id	stream path		
R100204	/var/audit_logs/old/NetguardID	NEWLINE	SPACE
R113203	/store/compressed/stat.log	NEWLINE	N A

Element Table 706

action id	element id	name	description	legal value	data unit	refresh period	sample period	period unit	aggregate
X200154	E312073	Date	Date of network transaction	DATE_ISO	N A	ASYN	SYNC	N A	N A
X200154	E312074	Time	Time of network transaction	TIME_24	N A	ASYN	SYNC	N A	N A
X200154	E312075	Action	Transaction Type	CHAR	N A	ASYN	SYNC	N A	N A
X200154	E312076	Source IP	Name of source firewall network interface	ALPHANUMERIC	N A	ASYN	SYNC	N A	N A
X200154	E312077	Destination IP	Name of destination firewall network interface	ALPHANUMERIC	N A	ASYN	SYNC	N A	N A
X200154	E312078	Source Address	Source IP address of packet	IP_4	N A	ASYN	SYNC	N A	N A
X200154	E312079	Destination Address	Destination IP address of packet	IP_4	N A	ASYN	SYNC	N A	N A
X200154	E312080	Protocol	IP protocol of packet	IP_4	N A	ASYN	SYNC	N A	N A
X200154	E312081	Source Port	Source port number / service name of packet or ICMP type	IP_PROTOCOL	N A	ASYN	SYNC	N A	N A
X200154	E312082	Destination Port	Destination port number / service name of packet or ICMP type	ALPHANUMERIC	N A	ASYN	SYNC	N A	N A
X200154	E312083	Packets Sent	Number of packets passed from source to destination	ALPHANUMERIC	N A	ASYN	SYNC	N A	N A
X200154	E312084	Packets Received	Number of packets passed from source to destination	UNSIGNED_INT_32	COUNT	ASYN	SYNC	N A	N A
X200154	E312085	Bytes Sent	Number of bytes passed from source to destination	UNSIGNED_INT_32	COUNT	ASYN	SYNC	N A	N A
X200154	E312086	Bytes Received	Number of bytes passed from source to destination	UNSIGNED_INT_32	COUNT	ASYN	SYNC	N A	N A
X317189	E444120	Date	Date of measurement	DATE_ISO	N A	ASYN	SYNC	N A	N A
X317189	E444121	Time	Time of measurement	TIME_24	N A	ASYN	SYNC	N A	N A
X317189	E444122	CPU Idle	Percent CPU Idle	PERCENT	PERCENT	1	10 MINUTE	AVERAGE	AVERAGE
X317189	E444123	System Percentile	Percent of CPU used for system tasks	UNSIGNED_INT_16	PERCENT	1	10 MINUTE	AVERAGE	AVERAGE
X317189	E444124	I/O Percentile	Percent of CPU used for I/O tasks	UNSIGNED_INT_16	PERCENT	1	10 MINUTE	AVERAGE	AVERAGE
X317189	E444125	User Percentile	Percent of CPU used for user tasks	UNSIGNED_INT_16	PERCENT	1	10 MINUTE	AVERAGE	AVERAGE

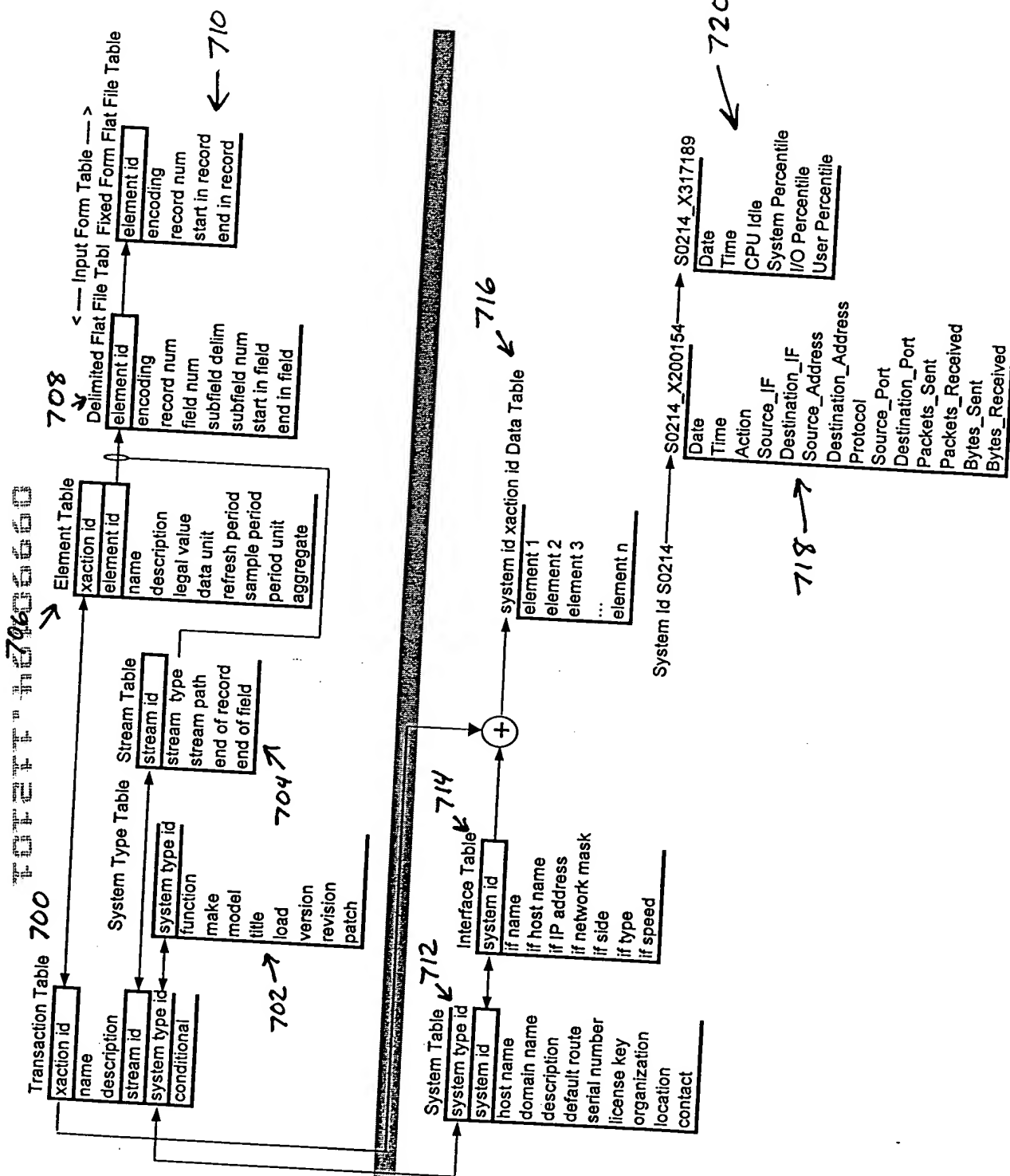
Delimited Flat File Table 708

element id	encoding	record num	field num	subfield delim	subfield num	start in field	end in field
E312073	ASCII_7_BIT		ALL	1 NONE	0	0	0
E312074	ASCII_7_BIT		ALL	2 NONE	0	0	0
E312075	ASCII_7_BIT		ALL	3 NONE	0	0	-1
E312076	ASCII_7_BIT		ALL	4 /	0	0	0
E312077	ASCII_7_BIT		ALL	4 /	1	0	0
E312078	ASCII_7_BIT		ALL	4 /	2	0	0
E312079	ASCII_7_BIT		ALL	5 NONE	0	0	0
E312080	ASCII_7_BIT		ALL	6 NONE	0	0	0
E312081	ASCII_7_BIT		ALL	7 NONE	0	0	0
E312082	ASCII_7_BIT		ALL	8 NONE	0	0	0
E312083	ASCII_7_BIT		ALL	9 NONE	0	0	0
E312084	ASCII_7_BIT		ALL	10 NONE	0	0	0
E312085	ASCII_7_BIT		ALL	11 NONE	0	0	0
E312086	ASCII_7_BIT		ALL	12 NONE	0	0	0
E312086	ASCII_7_BIT		ALL	13 NONE	0	0	0

Fixed Form Flat File Table 710

element id	encoding	record num	start in record	end in record
E444120	ASCII_7_BIT		ALL	1
E444121	ASCII_7_BIT		ALL	10
E444122	ASCII_7_BIT		ALL	12
E444123	ASCII_7_BIT		ALL	19
E444124	ASCII_7_BIT		ALL	21
E444125	ASCII_7_BIT		ALL	23
E444125	ASCII_7_BIT		ALL	24
E444125	ASCII_7_BIT		ALL	26
E444125	ASCII_7_BIT		ALL	27
E444125	ASCII_7_BIT		ALL	29
E444125	ASCII_7_BIT		ALL	30
E444125	ASCII_7_BIT		ALL	32

Figure 8




```
1999/10/2709:00:00043004010023
1999/10/2709:10:00022003005010
1999/10/2709:20:00043004010023
1999/10/2709:30:00043004010023
1999/10/2709:40:00043004010023
1999/10/2709:50:00043004010023
```

[illegible]

Figure 10

Date	Time	CPU Idle	System Percentile	I/O Percentile	User Percentile
1999/10/27	09:00:00	43	4	10	23
1999/10/27	09:10:00	22	3	5	10
1999/10/27	09:20:00	43	4	10	23
1999/10/27	09:30:00	43	4	10	23
1999/10/27	09:40:00	43	4	10	23
1999/10/27	09:50:00	43	4	10	23

Date	Time	CPU Idle	System Percentile	I/O Percentile	User Percentile
1999/10/27	09:00:00	43	4	10	23
1999/10/27	09:10:00	22	3	5	10
1999/10/27	09:20:00	43	4	10	23
1999/10/27	09:30:00	43	4	10	23
1999/10/27	09:40:00	43	4	10	23
1999/10/27	09:50:00	43	4	10	23